PCSRF Face-to-Face Meeting Notes

Thursday, June 12, 2003 8:30 AM – 5:00 PM ET
Hosted by National Institute of Standards and Technology
Gaithersburg, Maryland

Participants

Fred Proctor (NIST/MEL)
Keith Stouffer (NIST/MEL)
Joe Falco (NIST/MEL)
Art Griesser (NIST/EEEL)
Jerry Stenbakken (NIST/EEEL)
Tom Good (Dupont)
Dave Teumim (ISA)
Marv Schilt (Rockwell)
Michael McEvilley (DAC)
Lynne Ambuel (DAC)
Matt Franz (Cisco)
Dale Peterson (Digital Bond)
Michael Bush (Rockwell)
Holly Beum (Interface Technologies)
Diana McCormick (FCWA)
Marcus Berry (FCWA)
John Saunders (National Defense University)
Bill Miller (MaCT)
Joe Weiss (KEMA) – Conference Call
Jeff Dagle (PNNL) – Conference Call
Geoff French (Veridian) – Conference Call
Mark Godfrey (Conectiv)– Conference Call
Andrew Wright (Cisco) – Conference Call

Purpose

To share status and plans among participants; discuss and get comments on the new Security Capabilities Profile (SCP) for Industrial Control Systems document; determine possible scopes for Protection Profiles that will be generated from the SCP document; and plan the timing for the next meeting (conference call).

Web Site Updates

All information on the PCSRF site is password protected. If you don't have a username and password yet, please follow the directions located at http://www.isd.mel.nist.gov/projects/processcontrol/members.html to request one.

The following documents have been added to the PCSRF web site:

Security Capabilities Profile for Industrial Control Systems Document -
http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/SCP-13-June.doc

IEC 61508 Safety Standard Review
http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/61508_review.doc

May 22, 2003 PCSRF Conference Call Minutes
http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/22-May-2003.doc

SP99/PCSF Discussion

Dave Teumim opened the discussion with a slide on ISA SP99 and a slide on a security life-cycle model: http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/Presentations/SP99Lifecycle.ppt

Tom Good suggested that there are two industrial security needs that need to be addressed: installed base of equipment and future installations. SP99 should address the large installed base of equipment and how to apply security in the near term and that PCSRF should address what is needed in the future. There is about a 2 – 3 year R&D lag to develop new products.

Holly Beum added that WG1 and WG2 of SP99 are concerned with today's technologies and how they can be applied to current systems.

Michael Bush confirmed the 2 –3 year R&D lag and added that the vendors want standards to build to, not requirements. If there is nothing to build to, they will develop their own proprietary solution. Mike also mentioned that industries are developing their own standards such as SEMI 3507 - Provisional Specification for Equipment Client Authentication and Authorization.

Bill Miller added that everything can use PKI and that there is confusion around the adoption of the certificates.

Dale Peterson mentioned that according to the vendors that he deals with, selling certified products is a big thing and the sooner that there is something to certify products to, the better.

There were some discussions about producing best practices documents and Matt Franz added that their worst fear is that people don't adopt best practices.

Art Griesser mentioned that industry solutions today are tactical and the PCSRF work is strategic.

Mike Bush voiced that he still sees significant overlap between PCSRF and SP99 WG2.

Tom Good questioned if vendors are finding the efforts of PCSRF useful (ie. protection profiles).
Matt Franz said that they have people at Cisco to "decipher" Protection Profiles.

Michael McEvilley mentioned that a significant portion of the IEC 61508 safety standards document can be applied to what we are doing with security standards.

Security Capabilities Profile (SCP) Document Discussion

There have been two additional sector specific workshops to address vulnerabilities and security objectives:

- Pipeline sector (API) – held in Houston – Michael McEvilley attended (January 2003)
- Chemical sector – held at NIST (January 2003)

Information gathered from the sector specific workshops (oil -API, chemical, and discrete parts - NCMS) has been incorporated into the document.

The old SPS document has been revised into a new document:

- Renamed to "Security Capabilities Profile (SCP) for Industrial Control Systems"
- Includes info from the sector specific workshops (discrete parts, oil, chemical)
- Softened the text throughout to be less "security-ease"
- Added a section on how this document fits with various efforts (PCSRF, SP99, NIAP and other industry specific initiatives) and a diagram was included to illustrate the process within which this document fits.
- Added functional implementation requirements and assurance verification requirements

Michael McEvilley mentioned that the SCP is the forum's document and we are looking for feedback and suggestions to enhance the document.

Michael added that there are some limitations to the Common Criteria (CC) in that architecture, operations and maintenance are out of the scope of the CC

A topic of discussion of the group was the possibility of starting with component profiles and leaving the system level document (SCP) as is. There was some discussion as to where do we go from here and what does the group think of this plan for protection profiles.

Bill Miller suggested some possible components for PPs taken from the sections of the SCP document – Network Addressable Devices, Logging and Auditing systems, HMI

Mike Bush noted that analysis of the system is very important and that we have to get the system nailed before we can drill down to the component level.

Joe Weiss voiced that system security should take precedence over component level security

We need to perform risk analysis at the system level as well as the component level

Dale Peterson questioned that if we do PPs around components, will people be happy in the end?

Tom Good added that maybe we should target an element to write a profile for rather than a component.

Dale Peterson suggested that we may not be done identifying vulnerabilities yet.

The SCP needs some further review and enhancement. Dale Peterson suggested that we recruit a red team of good reviewers: candidates Tom Good, Dale Peterson, Bill Miller, Matt Franz, Holly Beum, Michael Bush, Joe Weiss.

Michael Bush voiced that we need to determine what are we trying to protect against. The main things that they are concerned about are: inadvertent actions, disgruntled employees, and hackers, in that order.

There was a discussion about whether the capabilities in the document are a minimal set of requirements or a superset of requirements. After some discussion, it was decided that they are a superset of requirements.

There was some discussion on developing a PCSRF roadmap to deploy security devices. It would be good to develop one PP to show progress and concrete the work.

The SCP should be distributed ASAP to the vendor community to get comments on it. There was some discussion as to whether SP99 can be used as a vehicle to distribute the SCP document to the community.

Develop use cases to get the point across to industry, vendors, etc. Fred Proctor added that pilot programs are very valuable

PCSRF Roadmap (Action Items)

1. Update the SCP draft (6/19)
2. Circulate new SCP draft for comment and review (competed by 7/8)
3. Determine if SP99 will act as a distribution vehicle for the SCP
4. Distribute the SCP to SP99 (7/15)
5. SCP/PCSRF presentation at ISA Houston (10/21 – 22)
6. Determine how to get vendors, etc to come to the ISA show
7. Next PCSRF conference call (mid August)
8. Best Practices for application areas – security levels
9. Pilot would be chosen from this best practices document

Testbed Tours

NIST has initiated the development of a security testbed comprised of several implementations of typical industrial control and networking equipment as well as relevant sensors and actuators. This industrial control security testbed is being used at NIST to develop test methods for validation and conformance testing of security implementations. The testbed is also being used to help identify system vulnerabilities as well as establish best practice guidelines.

Art Griesser Jerry Stanbakken gave a presentation and demonstration of the EEEL portion of the testbed, which is measuring the performance impact of adding encryption to SCADA links.

Keith Stouffer and Joe Falco gave a presentation and demonstration of MEL portion of the testbed.

There is a Power Point slide of the testbed available on the PCSRF site:
http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/Equipment_list_small.ppt

The testbed contains:

- Network hardware (firewalls, router, wireless access point, switches, modems, etc.)
- Industrial equipment (several PLCs and a DeltaV system)
- Flow meters, pumps, ultrasonic level sensors
- Conveyor system with DeviceNet

The testbed is being used at NIST to develop test methods for validation and conformance testing of security implementations. The testbed is also being used to help identify system vulnerabilities as well as establish best practice guidelines. NIST is looking for testable hardware.

Conference Call Updates

Jeff Dagle reported that there is a DOE RFP for cyber security of process controls. Proposals are due by the end of July. Jeff will be sending a draft proposal to the group for review and comment.

Joe Weiss noted that system security takes precedence over component level security

Next Meeting

The next PCSRF meeting will be a conference call in August 2003. Additional information, including agenda will be posted in the future.